

(19) 日本国特許庁 (J P)

(12) 公表特許公報 (A)

(11) 特許出願公表番号

特表平10-511783

(43) 公表日 平成10年(1998)11月10日

(51) Int.Cl.⁶

識別記号

F I

G 0 6 F 9/06
1/00
9/445
13/004 1 0
3 7 0
3 5 3G 0 6 F 9/06 4 1 0 B
1/00 3 7 0 B
13/00 3 5 3 V
9/06 4 2 0 J

審査請求 未請求 予備審査請求 有 (全 24 頁)

(21) 出願番号 特願平8-513861
 (86) (22) 出願日 平成6年(1994)10月24日
 (85) 翻訳文提出日 平成9年(1997)4月24日
 (86) 国際出願番号 PCT/US94/12222
 (87) 国際公開番号 WO96/13002
 (87) 国際公開日 平成8年(1996)5月2日

(71) 出願人 トレンド・マイクロ・インコーポレイテッド
 アメリカ合衆国カリフォルニア州95014,
 クパチーノ, スーツ・101, スティーブン
 ス・クリーク・ブルバード・202
 (72) 発明者 チャン, スティーブ, ミン・ヤン
 アメリカ合衆国カリフォルニア州90274
 ランチョ・パロス・ベルデス, イエロー・
 ブリック・ロード・6
 (74) 代理人 弁理士 古谷 馨 (外2名)

最終頁に続く

(54) 【発明の名称】 ワークステーションのブート前にネットワーク及びワークステーションのアクセスを制御する方法及び装置

(57) 【要約】

ローカル・エリア・ネットワーク上の、ワークステーション(13)と他のワークステーション(15)の間、またはワークステーション(13)とサーバ(11)の間でブート前ファイル及び情報を転送するための方法及び装置を提供する。ワークステーション・ブート・シーケンスの間に、ワークステーションとネットワークのオペレーティング・システムの様々な構成要素がロードされ実行される。ブート・シーケンスの後でワークステーションの全ての制御がワークステーションのオペレーティング・システムに渡されるので、ブートの後で実施されるいかなる管理作業もワークステーション上で稼働するアプリケーション・プログラム(23)によって実施されなければならない。本発明は、こうしたアプリケーション・プログラムの使用によって生じる問題を、例えば、個々のワークステーション(13)内にインストールされたLANカードの通常未使用のブートROMソケットに配置された適切なプログラムを含むROMまたはPROM(61)、または個々のワークステーションのマザーボードやシステム・ボード上に構築されたPROMやROM(61)を含むチップのようなハードウ

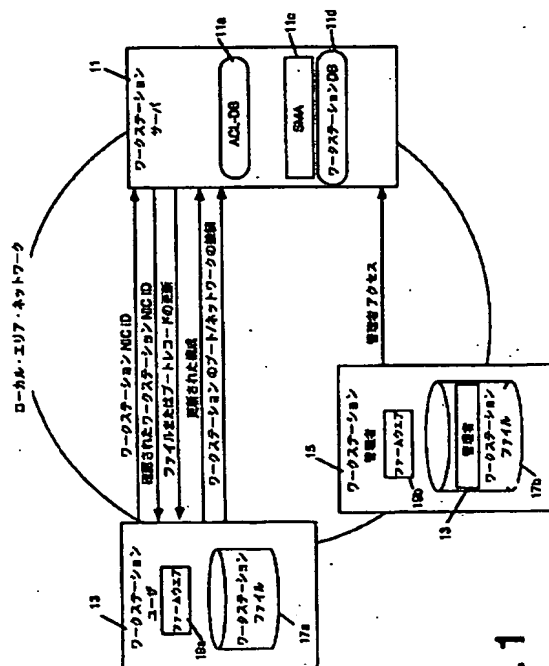


Fig. 1

【特許請求の範囲】

1. ワークステーションのオペレーティング・システムのロードが完了する前に、ネットワーク接続を介して所定のワークステーションの資源を制御できるようにした装置であって、前記装置が、

a) ワークステーションのスタートアップの際に動作可能で、ワークステーションのオペレーティング・システムを完全にロードする前に、ワークステーションのブート前処理から外部処理に制御を転送するための手段、

b) ネットワーク上のサーバに対するワークステーションのネットワーク接続を起動する手段、

c) ワークステーションのネットワークへの接続が認可されることを保証するために、ワークステーションの識別を認証する手段、

d) ワークステーション内の所定のファイルを、サーバ内のファイルに配置されたデータに基づいて更新する手段、及び

e) ワークステーションのオペレーティング・システムを完全にロードするために、ワークステーションのブート処理に制御を戻す手段を含むことを特徴とする、前記装置。

2. 制御を転送する前記手段が、プログラム・モジュールの存在を検出した際に制御が渡されるネットワーク・インタフェース・カードのROMソケット内に、プログラム・モジュールが存在することを検出する手段を含むことを特徴とする、請求項1に記載の装置。

3. ネットワーク接続を起動する手段が、

a) ネットワーク通信プログラムを記憶媒体からロードする手段、及び

b) 前記ネットワーク通信プログラムを実行し、前記ネットワークに接続されたサーバ内で実行されているサーバ管理アプリケーションとの接続を確立する手段を含むことを特徴とする、請求項1に記載の装置。

4. ワークステーションを認証する手段が、

a) ワークステーションにユニークな識別をネットワークを介してサーバに送信するよう命令する前記サーバ管理アプリケーションから命令を受信する手段、及

び

b) 前記サーバから、認可及び不認可のうち1つを受信する手段を含むことを特徴とする、請求項3に記載の装置。

5. ファイル更新手段が、前記認可が受信されたことを検出し、前記サーバからファイル更新情報を受信し、前記サーバへの前記更新が完了した際に確認を送信する手段を含むことを特徴とする、請求項4に記載の装置。

6. 制御を戻す手段が、ROMソケット内のプログラム・モジュールを終了させ、前記ワークステーションのブート処理に戻る手段を含むことを特徴とする、請求項1に記載の装置。

【発明の詳細な説明】

ワークステーションのブート前に、ネットワーク及び
ワークステーションのアクセスを制御する方法及び装置発明の背景

1. 発明の技術分野

本発明は、ローカル・エリア・ネットワーク (LAN) 内でワークステーションとして使用されるパーソナル・コンピュータに適用されるものである。

2. 発明の背景

ローカル・エリア・ネットワーク即ちLANとしてよく呼ばれるものを用いて、個々のパーソナル・コンピュータをワークステーションとして接続することは一般的なことである。LANは通常、コンピュータのネットワークとして定義され、オフィス・ビルの1つの階または複数階のような単一の地理的位置でケーブルやワイヤによって、様々な資源がワークステーション間で共有されるように、及び／または個々のワークステーションが電子メール即ちE-Mailを送受信できるように接続される。

通常、ローカル・エリア・ネットワークは、個々のユーザが別のサーバと呼ばれるコンピュータ、またはLAN上の他のワークステーションに物理的に関連するデータベースやファイルをアクセスできる

ようにする。この方法で、2人以上のユーザに必要とされるデータ及びプログラムは、ネットワーク上の単一コンピュータ上に維持され、依然としてネットワーク上の他のワークステーションで利用可能である。この例では、共通データを備えたコンピュータはサーバと呼ばれ、個々のユーザのワークステーションはクライアントと呼ばれる。他の例では、データベースやファイルが様々なワークステーション上でセットアップされ、それぞれがサーバとして機能し、かつクライアントとして機能しうる。これはピアトゥーピア (peer-to-peer) 構成と呼ばれることが多い。

数百または数千のワークステーションと数十のサーバの大きなネットワークでは、個々のワークステーションの統制、または管理は面倒な作業である。この管

理は、これに限られるものではないが、以下の作業からなる。

- ・ワークステーション構成制御
- ・システム・セキュリティ
- ・ワークステーション故障の復旧
- ・ソフトウェアのライセンス協定に関するアプリケーション監視
- ・ソフトウェア・アプリケーション分配
- ・ソフトウェア・バージョン制御
- ・ユーザ環境のカスタマイズ（例えば、メニュー、ブート・ファイル等）
- ・ユーザ訓練

こうした大きなネットワークでは、システム管理者がワークステ

ーションとして同じ物理位置内にいる必要があるので、この管理に非常に時間がかかり、退屈なものである。これらのワークステーションは、大きな複数階のビルのような広大な領域に亘って拡がるため、ワークステーション間を移動して管理作業を実施するのに非常に多くの時間と労力が費やされる。

また、これらの管理作業は、ワークステーションのブート（スタートアップ）サイクルの間に行われるコンピュータの機能に関連することが多い。それらは、構成の変更をテストするためにワークステーションの再ブートの繰り返しを必要とすることが多い。セキュリティの観点から、ワークステーションとサーバの両方のアクセスを制御する機能の多くは、ブート処理の前、間、及び後に行われる機能が制御できることで、大きく改善される。現在の方法は、ブート処理の間、及び後に行われる機能の制御に依存している。ワークステーションのブート前の多くの機能制御によって、ネットワーク管理者がワークステーションに対してかなり多くの制御を課すことができるために、ブート前の制御に関する方法が好ましいことがある。

本発明の簡単な概要

本発明は、ワークステーションと他のワークステーション、またはワークステーションとローカル・エリア・ネットワーク上のサーバとの間でのブート前ファイル及び情報の転送に関する方法と装置を意図したものである。便宜上、この説

明はDOSベースのシステムに関して行うものとする。しかし当業者には、本発明の概念がUNIXベ

ースのシステム及び他のネットワーク環境でのアプリケーションを有するものであることが認識される。特に、ネットワーク管理者が機能及び他のネットワーク管理作業を実施するメカニズムを提供することが必要である。そのメカニズムはワークステーションのブート前に課されなければならない。MS-DOS、PC-DOS、またはUNIXのようなその他の様々なオペレーティング・システムを使用するワークステーションは、ブート・シーケンスと呼ばれるスタートアップ処理を実行する。ブート・シーケンスの間に、ワークステーションとネットワークのオペレーティング・システムの様々な構成要素がロードされ実行される。ワークステーションの全ての制御が、ブート・シーケンスの後でオペレーティング・システムに送信されるので、ブート後に実行される全ての管理作業はワークステーション上で実行されているアプリケーション・プログラムによって実行されなければならない。これらのアプリケーション・プログラムはユーティリティと呼ばれることが多い。(ワード・プロセッサ、データベース管理、またはE-Mailのような)他のアプリケーションと同時にユーティリティを実行するためには、ユーティリティはワークステーションのメモリに常駐するようロードされなければならない。これは、利用可能なアプリケーションのメモリを少なくし、かつ、しばしばワークステーションを「ロックアップ」即ち「ハング」させる競合の原因となる。この場合、ワークステーションは再ブートされ、全てのプログラムが再ロードされなければならない。また、故障の間に使用されたデータを損傷したり喪失する可能性が高い。

本発明は、例えば個々のワークステーション内にインストールされたLANカードの通常未使用のブートROMソケットに配置された適当なプログラムを含むROMやPROM、または個々のワークステーションのマザーボードやシステムボード上に構築されたPROMやROMを含むチップといったハードウェア構成要素を提供することによって、これらの問題を克服する。PROM内のプログラムがセットアップされ、

システムのスタートアップ時に、ブート・シーケンスの間のワークステーションのオペレーティング・システム・ソフトウェアのロードの前に、そのプログラムが、ワークステーションの基本入出力システム (BIOS) を使用することによって一定のオペレーティング・システム機能を実施し、ワークステーションがネットワーク上のサーバと通信でき、ネットワークを介してワークステーションの必要資源をサーバ上で実行されているサーバ管理アプリケーションが利用できるようにする。システム管理者によって制御されるこの処理によって、様々なブート前機能がワークステーションで実施できる。

例えば、ワークステーション及びサーバのハードウェア内で符号化されるIDを交換することによって、ワークステーションがネットワークの接続に関して認可される。これは、ネットワークに大きく改善されたセキュリティを加える。また、他の例として、結果的に故障になる競合を起こしているワークステーションは、リモートで再ブートされ、その再ブート・サイクルの間に、競合の可能性をなくすようブート・ファイルが変更される。この処理は普通のものであるが、ワークステーションに座っている間常にオペレータ入力コ

マンドによって実行される。本発明はこの機能をリモートで実行できるようにする。本発明はまた、重要なブート・ファイルの使用に先立ち、それらのファイルをサーバから転送することによってワークステーションのブート前に重要なブート・ファイルのブート前更新をも提供する。ハード・ドライブのブート・セクタにウイルスの攻撃を受けたワークステーションは、抗ウイルス防御の多くの手段を提供するブート・シーケンスを実行する前に検出され修復されるダメージを有することがある。全てのブート前オペレーションがワークステーションのオペレーティング・システムのロード及び実行の前に行われるので、ワークステーションのハード・ディスク上に存在する可能性のあるアプリケーション、ユーティリティ、またはウイルスのような悪意のあるプログラムは本発明の制御下にある。

本発明は以下の理由によって高価値な技法として十分評価されうる。

- ・プロトコル及びオペレーティング・システムに依存する。
- ・要求時にのみ稼働する。

- ・TSRではないメモリを占有しない。
- ・システム管理者をサーバに接続させることができるツール。
- ・ローカル・ドライブがダメージを受けた場合、またはユーザがログインしない場合であっても、ブート時にワークステーションに対するネットワーク接続を構築可能である。
- ・ユーザの仲介なしにワークステーションのハード・ドライブにリモート・アクセスできる。

本発明によって可能な考えられるサーバ管理アプリケーションのいくつかの例は以下の通りである。

・構成管理（リモート編集及びワークステーションのシステム・ファイルのインストール）

- ・サービスの識別、及び認証
- ・スマート・ハブの管理
- ・クリティカル・ノードの監視
- ・ワークステーションのクラッシュの復旧
- ・リモートのソフトウェア・インストール、分配、監視、及び診断
- ・単一サインオン同期パスワード

最後に、本発明は以下の理由により様々なネットワーク管理の利点を提供する。

- ・ハングやクラッシュしたユーザ・ワークステーションへのアクセスを得るための「オフィスのハイキング」が必要ないので、年に数千時間が節減される。
- ・ユーザ・ワークステーションが中央で集中的に構成される。
- ・本発明が、環境に関わらず、適切なワークステーションの構成を可能にする。
- ・病的に振る舞うアプリケーションのためにTSRを許容できないユーザでも、本発明がTSRを必要としないために依然として利点を有する。
- ・ユーザとワークステーションの両方に対してブート前認証を加えることによって、セキュリティが大きく改善されうる。

・ソフトウェアのインストール、更新、バージョン制御、及び監視が著しく単純化され、集中化されうる。

・管理者のネットワーク全体の監視が大いに改善される。

簡単な図面の説明

図1は、1対のクライアント・ワークステーションと単一サーバを備えたローカル・エリア・ネットワークを示す全体ブロック図である。

図2は、本発明の一部を構成するPROMまたはROMに含まれるプログラムの機能構成要素を示すブロック図である。

図3a及び3bは、本発明で制御されるブート前シーケンスの流れ図である。

図4は、本発明のEE-PROM/ASICの実装を示すブロック図である。

発明の詳細な説明

図1は、単一サーバ・ワークステーション11、ユーザ13で示されたクライアント・ワークステーション、及び管理者15で示されたクライアント・ワークステーションを有するローカル・エリア・ネットワークを示す全体ブロック図である。サーバ・ワークステーション11は、サーバ・ファイル（図示せず）、アクセス制御リスト・データベース（ACL-DB）11a、及びNovellのNetWare環境におけるNetWareロード可能モジュール（NLM）のようなサーバ管理アプリケーション（SMA）を含み、これらは本発明に関連して機能し、データベース11dは、本発明によってブート前処理の間にワークステーション内の情報を変更するのに使用される情報を含む。クライアント・ワークス

テーション13及び15は同じ構成であり、それぞれはハードウェア構成要素（通常、PROMとASICの組み合わせで、ここではファームウェアと呼び、ワークステーションのインタフェース・ネットワーク・カードまたはマザーボード上にインストールされる）19a及び19bをそれぞれ含むが、管理者クライアントは管理者プログラム13も含む。このファームウェアは、完全にワークステーションのオペレーティング・システムがロードされる前に、ワークステーションの機能を管理し、サーバと通信する。

クライアント・ワークステーションのファームウェア（19aまたは19b）はまた

、クライアント・オペレーティング・システムのファイル・サービスへのブート前アクセスを提供し、クライアント・ワークステーションのオペレーティング・システム及びネットワーク・オペレーティング・システムのクライアント・ワークステーション構成要素の機能的部分集合を含む。その目的はサーバと通信することである。サーバ・ハードウェア構成要素は、サーバSMAから命令を取得する。サーバSMAは本発明のオペレーションを管理する制御ルーチンを含む。SMAへの好適なプログラムの組み込みに関する特徴は、実行するのが望ましい機能に依存する。しかし、こうした特徴は、ここで提供される記述に基づいて当業者が考えつくものである。管理的ユーティリティは、指示されたワークステーションで実行される。これらのユーティリティの1つは、管理者が一連のクライアントーサーバ・オペレーションをプログラムできるスクリプト言語であってもよい。

図1はクライアント・ワークステーション13とサーバ・ワークステーション11及びクライアント・ワークステーション15とサーバ・ワークステーション11の間の基本的な通信を示している。この（実際にネットワーク上で行われる）基本的な通信は、クライアントとサーバの接続を行うメカニズムを提供する。一旦その接続がなされると、クライアント13は、ファイル転送、ファイル更新、または（悪意の、または偶然のダメージによる）オペレーティング・システム救助のようなブート前機能が、SMAの制御のもとで自動的に行われる。

特に、クライアント・ワークステーションがネットワークに接続を試みる度に、ファームウェア19aまたは19bが、通信を行うべきネットワーク上のサーバを捜すプログラムを実行する。適当なサーバ、例えば、SMA（NovellのNetWare環境におけるNLM）を備えたサーバが、クライアント・ワークステーションに応答する。クライアント・ワークステーションが次に、本発明のサブシステムを使用して、そのネットワーク・インタフェース・カード（NIC）のアドレスをサーバに送信する。サーバSMAはそのアドレスをサーバに常駐するアクセス制御リスト11a内で確認する。サーバSMAは次に、実行するよう事前にプログラムされた作業を全て実行する。本発明は、SMAに常駐する限り便宜的技法であり、広範な様々のブート前サービスを提供するようカスタマイズ可能である。例えば、ファイル管理シ

システムはクライアント上で稼働しているため、ブートの前に新しいファイルをクライアントに転送することによって、ファイルを更新するようカス

タマイズできる。クライアントのブート・セクタがウイルスの感染がなく、ブート・セクタが完全な状態であることを確認するようカスタマイズすることができる。そうでない場合、ウイルスは除去され、ブート・セクタはサーバ上に常駐しているワークステーション・データベース11dから安全に復旧される。

一旦、全てのクライアントサーバのブート前機能が完了し、クライアントに知らされると、クライアント上の19aまたは19bがブート制御をクライアントのBIOSに戻す。クライアントは次に、通常の方法でブートを行い、完全にワークステーションのオペレーティング・システムをロードし、それが通常に行われた場合ネットワークに接続する。本発明のブート前シーケンスの利点は、クライアント・ワークステーションのブート、即ち通常ブートを中断し、またはよりダメージを与えるオペレーティング・システムに対する全てのダメージが、ブート前処理の間に管理され復旧されることである。本発明は、クライアント・ワークステーション内にインストールされた完全なオペレーティング・システムの機能的部分集合を含み、それによって、クライアントがダメージを被っているクライアント・ワークステーション内にインストールされたいかなるオペレーティング・システムの要素も使用することなく、無菌の環境から部分的にブートできる。この無菌環境は本発明のファームウェア内に維持される。第2の利点はクリティカル・ソフトウェア・システムに対するいかなる更新、復旧も、ユーザのいかなる使用も妨げないように無菌のオペレーティング環境を使用して集中して管理されうる

ことである。

サーバとのネットワーク接続を起動するための本発明の技法は、ワークステーション・ネットワーク・インタフェース・カード(NIC) ID(例えば、イーサネット環境ではイーサネット・ハードウェア・アドレス)のような登録されたユニークな識別を、標準あるいは事実上の標準ネットワーク・プロトコルを介してサーバに送信する。ネットワーク・プロトコルは、インターネットのTCP/IP、Novell

のNetWareのSPX/IPX、またはIEEEによって定義された任意の標準LANプロトコルのようなネットワーク環境に応じて変化する。サーバ・アプリケーションは事前に構成されたデータベースを検査して、接続が許可されるかどうか判定する。接続が確立された後、サーバSMAは、ワークステーションのファームウェア内のプログラムに適当な管理作業を実行するよう命令する管理要求を送信する。ファームウェアは実行されたオペレーションの結果をSMAに戻し、サーバによって認可された場合に通常のブート処理に戻る。

本発明はファームウェア（即ちPROMまたはROM内のプログラム）として実装されたクライアント・サーバ技法を使用し、それはオペレーティング環境に関わらずワークステーションで常駐終了型(TSR)を使用することなく任意のネットワーク・ワークステーションの完全なリモートのブート前制御を可能にする。本発明は、開発者及びOEMが注文によるサーバ・ベースのクライアント管理アプリケーションを構築できるオープン・アーキテクチャを提供する。

本発明の実装の一例は、必要なプログラム（即ちファームウェア）

を含む単一のPROMを使用し、それはASIC内に差し込まれてアドレスの復号化を提供し、このASICは、ほとんどのネットワーク・インタフェース・カード上の通常未使用のブートROMソケットに差し込まれる。必要なプログラムはファイル・ハンドラ、構成要素制御、ネットワーク・サービス、サーバ管理コマンド・インタフェース、及び実行可能サービス・エンジン機能を提供する。代替実施例では、このプログラムはフラッシュEPROMに含められ、これは当業者には明らかな理由によって、アドレス復号ASICを必要としない。

クライアント上のファームウェアは、顧客のアプリケーション・プログラム・インタフェース(API)またはSNMPのような業界標準プロトコルを介してサーバSMAと通信する。事実上、どんなサーバ管理アプリケーションも様々なプログラミング言語で書くことができ、また、既存のSNMP管理アプリケーションは直接アクセスできる。

本発明のPROMまたはROM内のプログラムの簡単なブロック図が図2に示されている。家事のサービス及び機能を除いてはこの説明に密接に関係しない。システ

ムは以下のものを含んでいる。

サーバ管理コマンド・インタフェース21：これはクライアント上のファームウェアとサーバ上のサーバ管理アプリケーション(SMA)の間の基本インタフェースである。その主な作業は、サーバSMAから送信されたパケット内のコマンドを解釈し、SMAに理解できる形式で、実行されたオペレーションの結果を含む応答パケットを構築することである。それは業界で定義された管理プロトコル、SNMPと同じ機能を果たす。

実行可能サービス・エンジン23：実行可能サービス・エンジンは、ワークステーションのブート前処理の制御を可能にする専用のブート前機能を提供する。実行可能サービス・エンジンはSMAの要求に基づいてその命令を受信する。言い換えれば、実行可能サービス・エンジンとSMAは一緒に、ワークステーションのブート処理が始まる前にワークステーションの行動を制御する。

オペレーティング・システム・カーネル25：オペレーティング・システム・カーネルは、実際は「ミニ・オペレーティング・システム」である。オペレーティング・システム・カーネルは、ファイル・ハンドラ27a、構成要素制御27b、及びネットワーク・サービス27cを使用し、インストールされたオペレーティング環境と適当に通信を行う。この環境は、ワークステーション環境(DOS、O/S2、UNIX等)とネットワーク・オペレーティング・システム(NetWare、LAN Manager、Vines等)の両方を含む。

サーバ管理コマンド・インタフェース21と実行可能サービス・エンジン23の機能を提供するのに必要なプログラムは、当業者には周知である。適当なオペレーティング・システム・カーネル25は、アメリカ合衆国デラウェア州WilmingtonのHitech Business Software, Inc. から入手可能である。

図3a及び3bは、システムのスタートアップ時におけるPROMまたはROM内のプログラムによって実行される処理のフローチャートである。

通常の実行オペレーションにおいては、図3a及び3bのフローチャートに示すように、本発明はBIOS(例えば、MS-DOS環境で)が実行され

た後ではあるがDOSの実行前に、ブート処理を遮断する。特に、ワークステーションの電源投入（ステップ31）の際、システムBIOSは当業者に周知の方法で実行される（ステップ33）。システムBIOSはネットワーク・インタフェース・カード上のROMソケット内のプログラムの存在を判定し（ステップ35）、制御をこのプログラムに渡す（ステップ37）。ここで図3bを参照すると、制御がPROM内のプログラムに渡されると、ネットワーク通信ソフトウェアが、ワークステーション記憶媒体から、その内部ミニ・オペレーティング・システムと適当なネットワーク通信プロトコルを使用してロードされる（ステップ39）。こうして、サーバSMAとの通信が起動される（ステップ41）。SMAからの命令のもと、本発明はPROM内のプログラムの実行可能サービス・エンジン内に含まれる適当な機能を実行する。実行可能サービス・エンジンは、DOSの下でのBIOSといった低レベルの制御機能を使用し、サーバSMAによってワークステーションに送信された命令を実行する。ステップ41でサーバ接続が起動された後、ワークステーションのNICアドレスが確認のためにサーバに送信される（ステップ43）。NICアドレスがACL-DB内がない場合（ステップ45）、ネットワークへの接続は切断され、そうでない場合、ワークステーションをネットワークに接続する試みがなされ（ステップ47）、それが成功するとワークステーション・ファイルが更新される（ステップ49）。成功しない場合、ネットワーク接続を起動する試みが繰り返される（ステップ41）。ステップ49で、サーバは任意の必要なワークステーションの更新をクライアントに送信し、SMAからの制御

のもとで任意の割り当てられた作業を実行する。ステップ49でワークステーション・ファイルを更新する間、PROM内にプログラムされた任意の処理が実行され、知らされる。この処理の実行と通知はサーバSMAからの命令のもとで、ファームウェアによって達成される。サーバとクライアントはワークステーションのハードウェアとファームウェアに通常の実オペレーティング・システムより下のレベルで直接通信し、そうして無菌の制御されたオペレーティング環境を提供する。クライアントによる更新の実施と通知（ステップ51）が成功した後、制御はワークステーション・ブート処理（ステップ53）に戻り、通常のブート処理が完了する

(図3aのステップ55)。ステップ39と41で述べた機能はファイル・ハンドラ27a及び27bによって実行され、ステップ43、45、47、49、51、及び53で述べた機能はネットワーク・サービス27cと実行可能サービス・エンジン23によって実行される。

ファームウェア内のオペレーティング・システム・カーネルがワークステーションを制御し続けているので、元のオペレーティング環境が存在する。ワークステーションはSMAによって送信されたいかなる命令も実行でき、ファームウェアの制御を終了し、通常のブートを開始できる。SMAによるブート前処理の間にされる任意の変更が、ワークステーションで即座に反映される。

図4を参照すると、ファームウェア19aと19bが、256KのPROM 61のような読み取り専用メモリ (ROM) 上に実装される。図4に示すように、必要なものには、ワークステーションが最初にセットされ、または

ハードウェアが追加された場合に、ユーザによってセットアップされるワークステーション構成メモリとして機能する、2Kの（あるいはそれ以上の）EE-PROMまたはRAM 63もある。本発明の目的に関し、このメモリ内に記憶される必要のある情報は、ネットワーク上の他の装置と通信する必要がある、ワークステーション・ディスク・ドライブまたは他の記憶媒体上のネットワーク・ドライバ・プログラムだけである。前述したように、このような実装がされると、ページ制御65を備えたアドレス復号器も必要になってくる。アドレス復号器ロジックは、共有メモリのページング・ロジックを提供する。これは、ブートPROMが8Kバイトのアドレス指定可能メモリ空間だけしか提供できないので、通常のDOSシステムには必要である。本発明に必要な256Kのメモリ空間にアクセスするために、アドレス復号器ロジックが必要で、それはROMアドレス空間をワークステーションのCPUにアクセス可能な8Kのページにページングする。アドレス復号器の機能がASICを使用して提供されることが望ましい。ネットワーク・インタフェース・カードに差し込むことができ、本発明が使用するプログラムを含むPROMを差し込むことができる適当なASICを製造するための詳細は、当業者には明らかである。

ファームウェア内にプログラムされたブート前機能の更なる例のいくつかは、

クライアントが最新バージョンのアプリケーション・ソフトウェアのみで稼働しており、ウイルス・スキャナに関する最新のデータベースがそのクライアントで利用可能であり、かつ正しいブート・ファイルがそのクライアントの所定の位置にあることを

保証するよう検査するものである。ブート前処理の間にエラーが見つかったら、PROMのプログラムはサーバ・ファイルから適当な更新を行う。

しかし、本発明の目的に関して、潜在的にカスタマイズされる機能は考慮されていない。本発明によるブート前に使用されるクライアント内にある基本的で便宜的な技法が請求の範囲に記載される。

【図1】

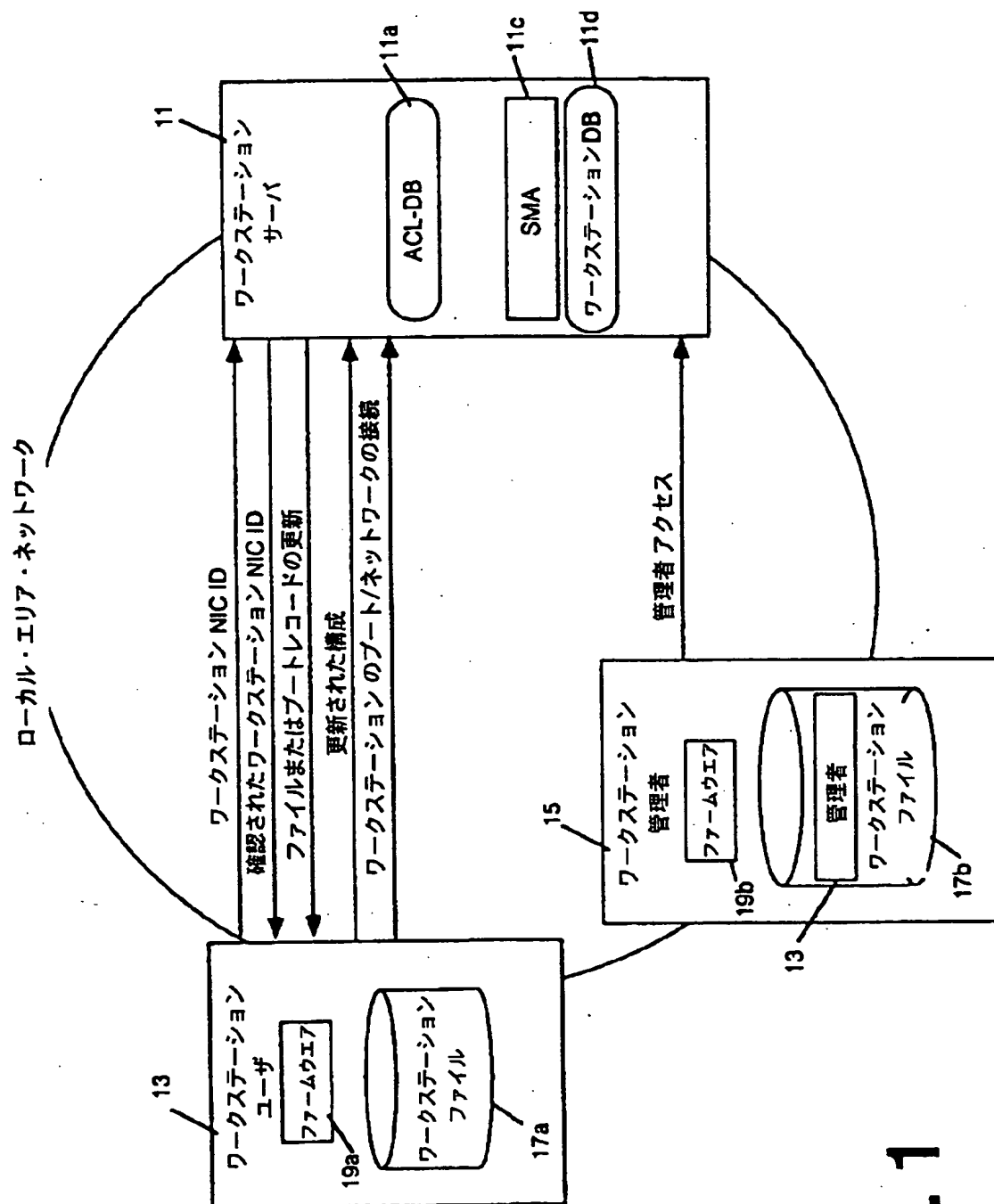


Fig. 1

【図2】

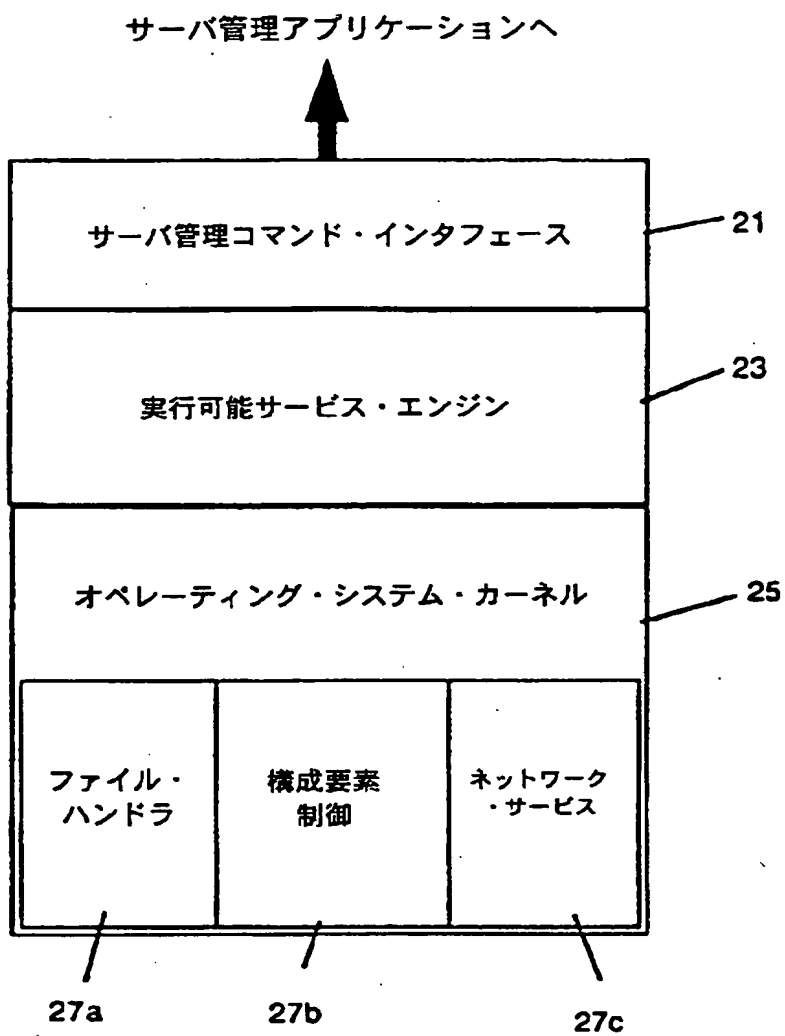


Fig. 2

【図3】

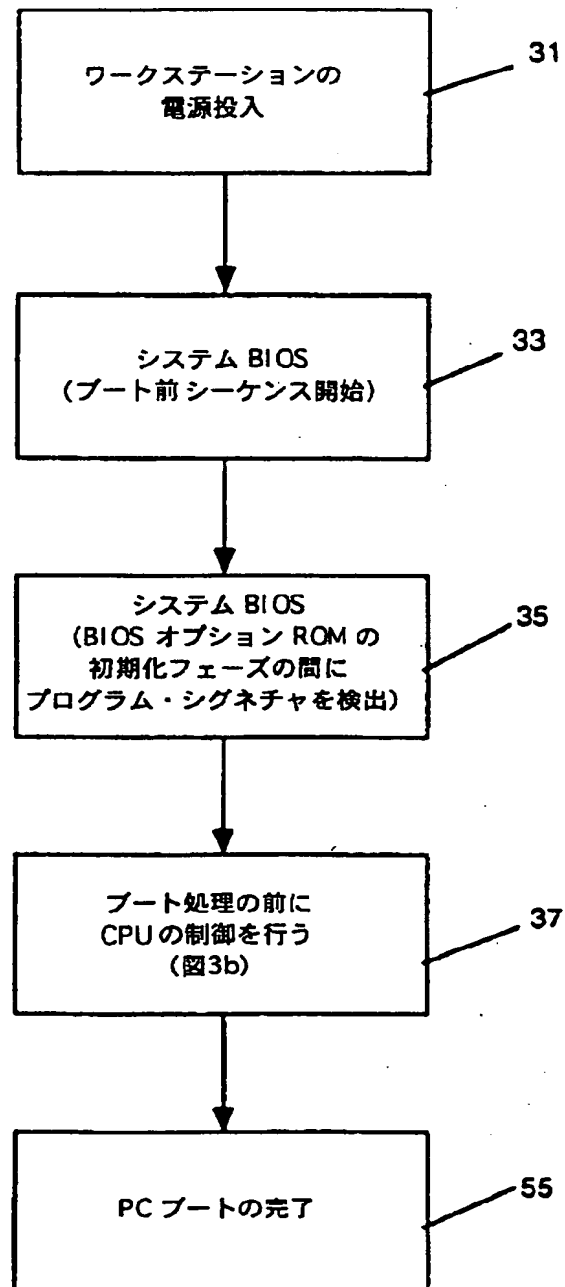


Fig. 3a

【図3】

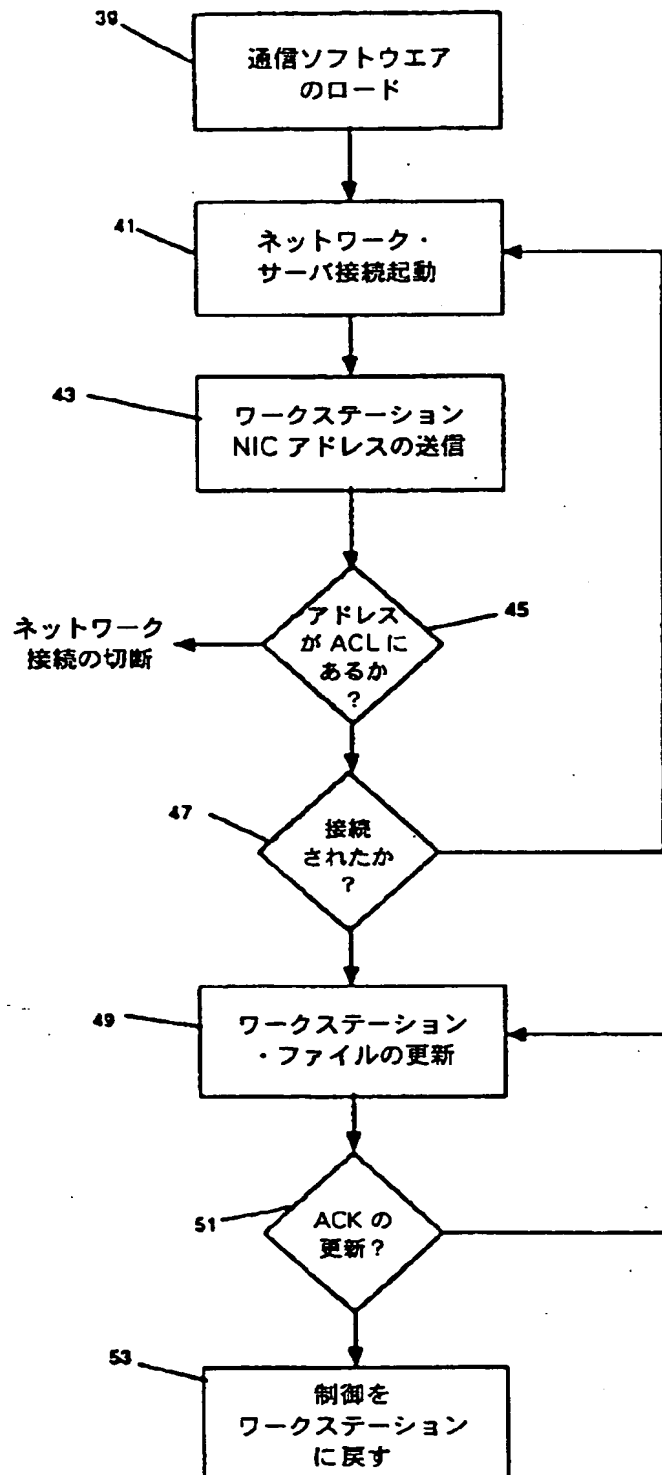


Fig. 3b

【図4】

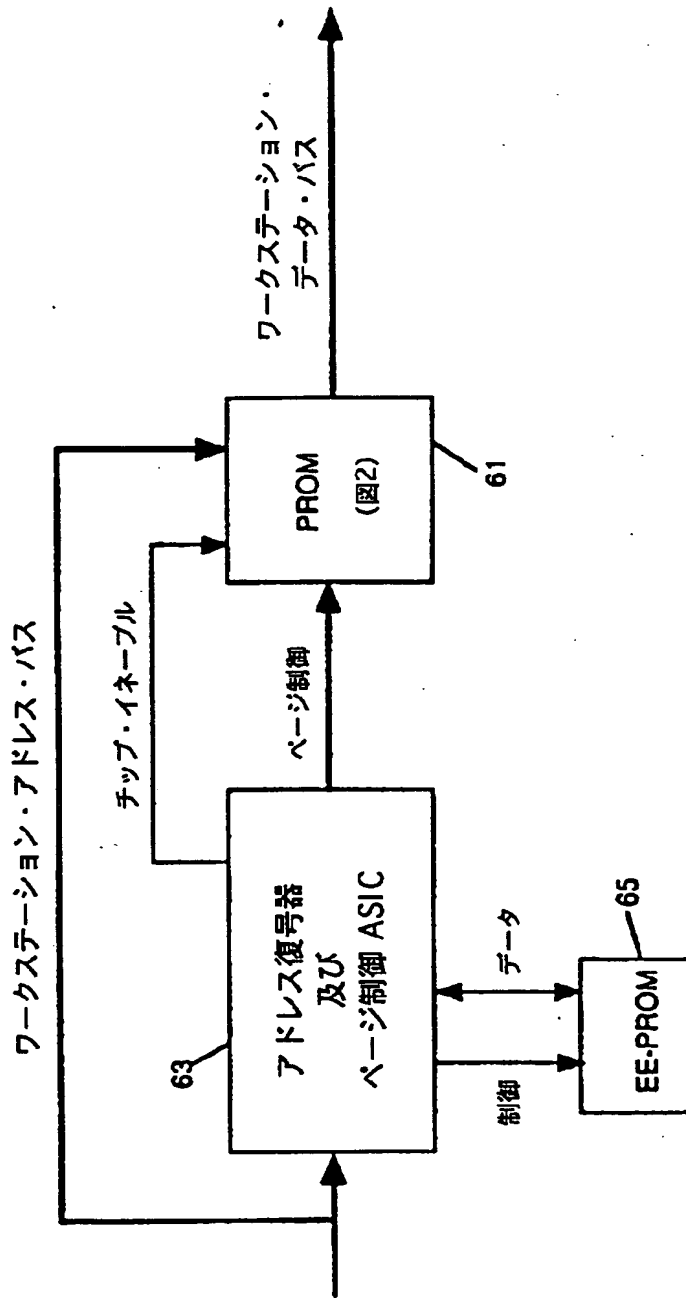


Fig. 4

【國際調查報告】

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US94/12322

A. CLASSIFICATION OF SUBJECT MATTER IPC(6) : G06F 9/445, 1/24 US CL : 395/700, 200 According to International Patent Classification (IPC) or to both national classification and IPC		
B. FIELDS SEARCHED Minimum documentation searched (classification system followed by classification symbols) U.S. : 395/700, 200, 325, 575; 380/25, 49 Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)		
C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US, A, 5,138,712 (Corbin) 11 August 1992, Figs. 1-4c, and abstract.	1
A	US, A, 5,121,345 (Lentz) 09 June 1992, Figs. 1-2 and abstract.	1-6
A	US, A, 4,982,430 (Frezza et al.) 01 January 1991, Figs. 1-3 and abstract.	1
A	US, A, 5,146,568 (Flaherty et al.) 08 September 1992, Figs. 1-3e and abstract.	1-6
A	US, A, 4,590,557 (Lillie) 20 May 1986, Figs. 1-4b and abstract.	1-6
<input checked="" type="checkbox"/> Further documents are listed in the continuation of Box C. <input type="checkbox"/> See patent family annex.		
* "A"	Special categories of cited documents: document defining the general state of the art which is not considered to be part of particular relevance	"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"E"	earlier document published on or after the international filing date	"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another claim or other special reason (as specified)	"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"O"	document referring to an oral disclosure, use, exhibition or other means	"Z" documents member of the same patent family
"T"	document published prior to the international filing date but later than the priority date claimed	
Date of the actual completion of the international search 06 JANUARY 1995		Date of mailing of the international search report 12 APR 1995
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230		Authorized officer KRISNA LIM <i>B. Nayak for</i> Telephone No. (703) 305-9672

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US94/12222

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US, A, 5,325,529 (Brown et al.) 28 June 1994, Figs. 3a-a5 and abstract.	1-6
A	US, A, 5,237,690 (Bealkowski et al.) 17 August 1993, abstract	1
A	US, A, 5,247,659 (Curran et al.) 21 September 1993, Figs. 1-5 and abstract.	1-6
A	US, A, 5,261,104 (Bertram et al.) 09 November 1993, Figs. 1-5 and abstract.	1-6
A	US, A, 5,276,863 (Heider) 04 January 1994, Figs. 1-3 and abstract.	1-6
A	US, A, 5,280,627 (Flaherty et al.) 18 January 1994, Figs. 1-3c and abstract.	1-6
A	US, A, 5,325,532 (Crosswy et al.) 28 June 1994, Figs. 1-8 and abstract.	1-6
A	US, A, 5,073,933 (Rosenthal) 17 December 1991, Figs. 1-3 and abstract.	1
A	US, A, 5,204,897 (Wyman) 20 April 1993, Figs. 1-7 and abstract.	1-6

フロントページの続き

(81) 指定国 EP (AT, BE, CH, DE, DK, ES, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OA (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG), AP (KE, MW, SD, SZ), AM, AT, AU, BB, BG, BR, BY, CA, CH, CN, CZ, DE, DK, EE, ES, FI, GB, GE, HU, JP, KE, KG, KP, KR, KZ, LK, LR, LT, LU, LV, MD, MG, MN, MW, NL, NO, NZ, PL, PT, RO, RU, SD, SE, SI, SK, TJ, TT, UA, UZ, VN

【要約の続き】

エア構成要素を提供することによって解決する。PROM (61) にプログラムがセットアップされると、システムのスタートアップ時 (31) において、ブート・シーケンスの間にワークステーションのオペレーティング・システム・ソフトウェアがロードされる前に、ワークステーションの基本入出力システム (BIOS) を使用して一定のオペレーティング・システム機能 (35) を実行し、ワークステーションがネットワーク上のサーバと通信することを可能にし、そのネットワークを介して、サーバ上で動作しているサーバ管理アプリケーション (11c) がワークステーションの必要な資源を利用できるようになる。この処理は、システム管理者 (15) によって行われ、様々なブート前機能をワークステーションで行うことができる。